copy to D.D (CSA)
14/8.

15(I)

TOP SECRET

TICOM/I-67

PAPER BY DR. OTTO BUGGISCH OF
OKH/IN. 7/VI AND OKW/CHI ON
CRYPTANALYTIC MACHINES

Attached is the translation of a write-up done at REVIN in August 1945 by Dr. BUGGISCH on the employment of Cryptanalytic Machines by IN. 7/VI and OKW/Chi in so far as he knew about them.

TICOM

13 August 1945

No. of pages: 4

Distribution:

British

Director
D.D.3
D.D.4
D.D. (N.S.)
D.D. (M.W.)
D.D. (A.S.)
A.D. (C.C.R) (2)
Lt. Col. Leathem

U.S.

OP 20-G (2) (via Lt. Pendergrass)
G-2 (via Lt. Col. Hilles)
S.S.A. (2) (Via Major Seaman)
Director, S.I.D. USFET
(via Lt. Col. Johnson)

TICOM

Chairman
S.A.C. (2)
Cdr. Bacon
Cdr. Mackenzie
Cdr. Tandy
Lt. Col. Johnson
Lt. Col. Lewis Powell
Lt. Cdr. Manson
Major Seaman
Major Morgan
Lt. Vance
Capt. Cowan
Lt. Fehl
Ticom Files (2)

Additional

Mr. Twinn
S.A.C. for Mr. Freeborn

PAPER ON CRYPTANALYTIC MACHINES

AT OKH/IN 7/VI and at OKW/Chi.

At Hollerith department was set up at IN 7/IV (later IN 7/VI and then Ag N/NA) as early as the Winter of 39/40. This was done at the instigation of some actuaries who were familiar with cryptanalytic problems there and knew Hollerith methods from civil life. The Hollerith section grew considerably in the course of time, both in respect of the number of machines it had and of personnel engaged. In 1943 there were perhaps 30-40 female punchers engaged and about 20-30 soldiers who were Hollerith mechanics and such like in civilian life. Baurat Schencke was in charge. Some of the bigger Hollerith machines were always being provided with special new wirings for special cryptanalytic purposes, as e.g. for non-carrying addition and subtraction in codes work. Most of the tasks, however, consisted of the usual statistics (bigrams, trigrams, chain statistics, [Kettenstatistic], column statistics [Spaltenstatistic] and of simple figure-calculations, e.g. in work on Hagelin machines. But, as a rule, no tasks were undertaken which could not have been carried out by hand by perhaps 100 people in a reasonable time.

The limited width of the Hollerith card was soon found to be inconvenient, particularly in counting out of repeats for the purpose of lining-up [Vergatterung] 2 cipher texts. The obvious solution appeared to be in this case to work with perforated strips and 5-unit alphabet. Orders were given at the beginning of '43 (?) for the construction of such a machine. As, however, section VI only had a completely inadequate workshop at its disposal, and by that time it was already impossible to get any more tools etc., an agreement was made with the Hollerith firm that a few rooms, together with workshop machines, tools etc., in the factory buildings at Lichterfelde Ost should be placed at the disposal of section VI. An engineer of the name of Schuessler of the Hollerith firm was placed in charge of this newly set-up workshop; he was dressed up as a Sonderfuehrer (Z), and was given a special section of his own. He was, in my opinion, pretty unsuitable for solving the problems set and, anyway, as far as his specialist knowledge was concerned, not even remotely comparable to the undermentioned gentlemen of OKW/Chi. The repeat counting machine was ready in the Autumn of '43 (or Winter 43/44?). It worked on a mechanical-electrical principle, the speed was not very high (I think a maximum of 40 pairs of letters a second), and there was somehow an "idling period" [Leerlauf] which was very inconvenient. It is worth noting that, when this apparatus was completed, none of the specialist department doing practical cryptanalysis had any use for it, so that the question was justifiably raised why such an apparatus had been built at all. I do not think that it was ever used for practical tasks.

In the Winter '43/44, the workshop began to be engaged on the construction of various mechanical aids, but they cannot be described as cryptanalytic machines. Thus, for example, a machine was made which automatically punched on Hollerith cards the Russian T/P traffic taken on perforated strips with 5-unit alphabet. Plans were made, too, in the Spring of '44 for machines which were to perform certain calculation tasks such as arose during work on Hagelin machines; but those were not cryptanalytic machines either, but special calculating machines. I do not know whether work was ever started on the construction of these machines - the order was probably issued - because I went to an entirely different department in June '44 and was given quite different tasks. In short, Ag N/NA had until June '44, and in all probability subsequently, no cryptanalytic machine which could be used for the practical solution of any codes or ciphers.

Things were different at OKW/Chi. There was no Hollerith department there (as far as I know), and perhaps for that very reason they felt, more

than in IN 7-Ag N, the necessity of developing and constructing special devices. I should think it was in the Summer of '42 that I heard for the first time that Chi had a workshop for special purposes of this kind and that, in particular, a repeat-counting apparatus was being constructed there, bearing the nick-name "Sawyers Jack" [Saegebock]. In the year '43, some gentlemen of our section VI visited the Chi workshop: among these was Doering, who told me that other devices in addition to the Saegebock were being constructed (or were even already in existence ??) and that clearly first-class specialists were working there. Then again in the Summer of '43, I paid another visit to Chi on other business and had a discussion with Oblt. Hasenjaeger, who belonged to Dr. Huettenhain's specialist party. In the course of this meeting, he told me that it was possible to construct repeat counting devices with a capacity of 10,000 pairs of letters a second (?), attained by means of using photo-electric cells which worked for all intents and purposes without inertia. Films were probably to be used as carriers of the cipher texts. He also said that Chi was considering the possibility of constructing such a high-performance device.

It was not until March or April '44 that I myself saw anything of the devices at Chi. I was there for a short time, for a reason which I no longer remember, to see Dr. Huettenhain, and while I was there Fregattenkapitaen Singer of Skl/MND by chance arrived too. On this very morning, General Fellgiebel was expected to come and see the devices; and they were all set up ready to work. Dr. Huettenhain arranged for Kap. Singer and me to be shown the devices by the director of the workshop, Dipl. Ing. Rotscheidt (I am not sure of the spelling). There was only a very short time for this, (1/4 to ½ hour), as the General was expected any moment. I clearly remember 3 devices :

1) Repeat counting device.

This was not the above-mentioned high-performance device, which clearly had not yet been constructed. I do not remember the number of pairs of letters read per second, but it cannot well have been more than 100. The device worked with perforated strips and photo-electric cells (?).

2) Device for solving simple transpositions.

The cipher text was slid along itself; any favourable positions which appeared during this process were marked on a strip. The figures which were produced were termed "Warships" (or was that on another device ?). It was not explained how the evaluation of the places was done. From my, it is true very limited, experience in the field of transposition sliding, I could not quite see how they could achieve their aim in this way. Nevertheless, it was maintained that a Japanese transposition system had been worked on with success with this device.

4)[sic] Device for recovering a figure subtractor in 4-figure codes.

I had not properly understood the principle at that time, but there was no time to ask questions. There was a square of 100 x 100, corresponding to the 10,000 possible, book-groups, against which in some way the cipher text groups were placed. The system worked optically, after some operations or other the square was photographed and the point of deepest black looked for: that gave the result. There was no corresponding system for a 5-figure code.

Apart from these, there were one or two devices there which worked out

some sort of statistics. One, I remember, looked for repeats, which were recorded automatically. The perforated strip with 5 unit alphabet was on all the devices with the exceptions of 3) the carrier of the cipher text, if I remember rightly. A large number of relays was used, and in addition, photo-electric cells and possibly condensers too as storers. Kap. Singer spoke briefly with Baurat Rotscheidt on some purely technical matters, of which I understood nothing. I never had a chance to put any questions. I do not know what codes and ciphers were really worked on by means of these machines - apart from a reference to the Japanese transposition system. I should think they were diplomatic traffics, in accordance with the sphere of Chi. Some of the workshops in which the devices were constructed were in the building, some in Grunewald, and some at Jüterbog. I heard and saw nothing more of all these devices later, as I have been working on nothing but ciphering since June. I did, however, speak to Dr. Rotscheidt two or three times about this new activity since he was interested in it. In the Winter, he even spent a few hours once at Signals Experimental Station Staats, in order that Dr. Lotze could show him the devices they had for deciphering enciphered speech.

Trans: K.C.K.